AUDIT AND ACCOUNTABILITY

Effective Date	*1/29/2020*
Policy Number	*TEC-PL-104*
Sponsor	*Chief Information Officer (CIO)*
Responsible Office	*Information Technology Services (ITS)*
Next Review Date	*1/29/2024*

I. REASON FOR POLICY

This Event and Transaction Audit and Accountability Policy establishes a process to ensure an effective event and transaction audit and accountability program designed to help manage the risks of inadequate event logging and transaction monitoring, to aid in the proper retention of audit evidence.

The State University of New York at Fredonia (*"Fredonia"*) Event and Transaction Audit and Accountability Policy serves to be consistent with best practices associated with organizational Information Security management. This policy establishes the requirement of an audit and accountability process throughout Fredonia and its Functional/Business Units to help the organization implement security best practices with regard to event and transaction documentation (logging), and the retention of audit evidence.

Each Fredonia Functional/Business unit is bound to follow this policy, and must develop or adhere to a program plan which demonstrates compliance with the standards enumerated within the policy.

This Policy is based on the Audit and Accountability principles established in NIST SP 800-53 “Audit and Accountability Control Family guidelines.”

This policy establishes the requirement of an audit and accountability process throughout Fredonia and its Functional/Business Units to help the organization ensure that there is adequate event and transaction documentation (logging), and the retention of audit evidence for purposes of demonstrating efforts related to events and transactions.

II. POLICY STATEMENT

It is the policy of Fredonia to establish and adhere to an Event and Transaction Audit and Accountability process meant to ensure that notable information security and information technology events and transactions are adequately documented/logged. The purpose of an Event and Transaction Audit and Accountability process is to help manage the risks associated with inadequate event logging and transaction monitoring, and to aid in the proper retention of audit evidence. Each Fredonia Functional/Business Unit utilizing Fredonia Information Assets, Business Systems, and Information Technology Resources must adhere to the event and transaction audit and accountability process outlined in this Policy, and must develop or adhere to a program plan that demonstrates compliance with the standards enumerated in this Policy.

This policy is applicable to all Information Assets, Business Systems, and Information Technology Resources owned and/or operated by Fredonia. Any information, not specifically identified as the property of other parties, that is transmitted or stored on Fredonia IT resources (including e-mail, messages and files) is the property of Fredonia . All users of IT resources, including Fredonia employees, contractors, vendors or others, are responsible for adhering to this policy.

All Fredonia Functional/Business Units must take action to implement the Access Control steps outlined in the NIST SP 800-53 “Audit and Accountability Control Family guidelines” in accordance with this Policy. Unless otherwise directed by Federal regulation relating to the implementation of the NIST SP 800-171 requirements, all controls will be implemented in accordance with the “LOW” baseline standard.

NOTE: The Information Technology Services (ITS) department will generally be the primary implementers of these controls however, any employee or affiliate utilizing University regulated data and/or system(s) will need to adhere to the policy requirements.

1. Audit and Accountability Procedures: (AU-1):

   Fredonia:

   a. Develops, documents, and disseminates to Fredonia employees and Affiliates that utilize University regulated data:

      1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and

   b. Reviews and updates the current:

      1. Audit and accountability policy annually and

      2. Audit and accountability procedures as needed.

2. Auditable Events: (AU-2)[1]:

   Fredonia:

   a. Determines that the information system is capable of auditing the following events: password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, Personal Identity Verification credential usage, or third-party credential usage;

   b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

   c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

   d. Determines that the following events are to be audited within the information system:

      password changes: each event, failed logons or failed accesses related to information systems: each event, administrative privilege usage: each event, Personal Identity Verification credential usage: each event, or third-party credential usage.

3. Content of Audit Records: (AU-3)[1]:

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event

4. Audit Storage Capacity: (AU-4)[1]:

Fredonia allocates audit record storage capacity in accordance with SUNY Records Retention.

5. Response to Audit Processing Failures: (AU-5)[1]:

The information system:

a. Alerts System Custodian in the event of an audit processing failure; and

b. Takes the following possible additional actions: shut down information system, overwrite oldest audit records, stop generating audit records.

6. Audit Review, Analysis, and Reporting: (AU-6)[1]:

Fredonia:

a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of malicious login attempts, tampering of information systems, login attempts from unauthorized locations, and information access anomalies; and

b. Reports findings to an Information Security Office personnel.

7. Audit Reduction and Report Generation: (AU-7)[1]:

The information system provides an audit reduction and report generation capability that:

a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and

b. Does not alter the original content or time ordering of audit records.

8. Time Stamps: (AU-8) 1:

The information system:

a. Uses internal system clocks to generate timestamps for audit records; and

b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets clocks synchronization within hundreds of milliseconds.

9. Protection of Audit Information: (AU-9)[1]:

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

10. Non-Repudiation: (AU-10):

The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed information sharing, sending and receiving of messages, approving of information.

11. Audit Record Retention: (AU-11):

Fredonia retains audit records in accordance with the New York State Records Retention Schedule to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

12. Audit Generation: (AU-12):

The information system:

a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components];

b. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and

c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

[1] Note: This 800-53 security control directly relates to CUI security requirement 3.3 Audit and Accountability specified in the 800-171 document.

III. RELATED DOCUMENTS, FORMS AND TOOLS

SUNY Procedure, Information Security Guidelines, Procedure Document 6608.

OTHER RELATED INFORMATION

The following are references to related Federal and State laws, policies, guidelines, and resources on cyber security.

Federal NIST National Institute of Standards and Technology, U.S. Department of Commerce, Information Technology Laboratory, Computer Security Division, Computer Security Resource Center.

- NIST 800-53
    - NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, Joint Task Force Transformation Initiative, April 2013.
        - Summary: To achieve a more secure information systems and effective risk management, document provides “guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the requirements of FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems.”
    - Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Computer Security Division, February 19, 2014.
        - Summary: Provides an overview of NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, which was published April 30, 2013.

  - NIST Special Publication 800-53, NIST SP 800-53 database of security controls and associated assessment procedures defined in NIST SP 800-53 Revision 4, Recommended Security Controls for Federal Information Systems and Organizations.
    - Security Controls and Assessment Procedures for Federal Information Systems and Organizations - Control Families, NIST Special Publication 800-53 (Rev. 4).
      - AC - Access Control
      - AU - Audit and Accountability
      - AT - Awareness and Training
      - CM - Configuration Management
      - CP - Contingency Planning
      - IA - Identification and Authentication
      - IR - Incident Response
      - MA - Maintenance
      - MP - Media Protection
      - PS - Personnel Security
      - PE - Physical and Environmental Protection
      - PL - Planning
      - PM - Program Management
      - RA - Risk Assessment
      - CA - Security Assessment and Authorization
      - SC - System and Communications Protection
      - SI - System and Information Integrity
      - SA - System and Services Acquisition
- NIST 800-100
  - Special Publication 800-100, Information Security Handbook: A Guide for Manager, United States Department of Commerce National Institute for Standards and Technology (NIST), October 2006.
    - Summary: Written for the federal sector, but provides guidance on a variety of other governmental, organizational, or institutional security requirements. Within the document, it informs information security management teams (CIOs, CISOs, and security managers) about various aspects of information security that they will be expected to implement and oversee in their respective organizations, and provides guidance for facilitating a more consistent approach to information security programs across the federal government.
- NIST 800-92
  - Special Publication 800-92 Guide to Computer Security Log Management, United States Department of Commerce National Institute for Standards and Technology (NIST), September 2006.
    - Summary: Assists organizations in understanding the need for sound computer security log management and provides practical guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise.
- NIST 800-171

- NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, June 2015.

New York State

- New York State Information Technology Standard Number: NYS-S14-005, Security Logging Standard.
    - Available at: https://www.its.ny.gov/document/security-logging-standard.

IV. DEFINITIONS

TERM	DEFINITION

Business Systems	Any and all Information Technology (IT) resources and information assets owned and/or operated by Fredonia .
Functional/Business Unit	This term used throughout the policy refers to each and every functional, department, and office unit within Fredonia, from the Provost area, to HR, to Finance, to ITS, and on and on.
Information Asset	This term used throughout the policy refers to Fredonia's information assets. Fredonia creates, possesses, and manages information. This information is Fredonia property with a financial value. The term "information asset" refers to the information that Fredonia has in its possession that had value to the institution. That value of information increases based on the value that the information has to Fredonia, both as property, and as a tool to allow Fredonia to operate its Information Assets, Business Systems, and Information Technology Resources and Functional/ Business units.
Information Technology (IT) Resources	This term used throughout the policy refers to Fredonia's information assets (i.e. hardware, software, or data). Fredonia creates, possesses, and manages information. This information is Fredonia property with a financial value. The term "Information Resources" refers to the information that Fredonia has in its possession that had value to the institution. That value of information increases based on the value that the information has to Fredonia, both as property, and as a tool to allow Fredonia to operate its Business Systems and Functional/ Business units.
Event and/or Transaction	For purposes of this Policy, an "event" or "transaction," at a minimum, will always include the following: ● User Access within a Business System ● User Transactions with respect to access of Information Assets, Business Systems, and Information Technology Resources ● Any technology access events or transactions specifically designated by the Functional/Business Unit as a circumstance which rises to the level of an "event" or "transaction" worthy of documentation in the form of access logs, documented access transactions, or other access to information assets that is recorded for purposes of audit and accountability.

V. CONTACT & ENFORCEMENT

ROLE	CONTACT	PHONE	EMAIL - Website
Responsible Office	Information Technology Services	(716) 673-3407	tracker@fredonia.edu
Enforcement	Human Resources	(716) 673-3434	human.resources@fredonia.edu
Policy	University Policy Office	(716) 673-4828	policy@fredonia.edu policy.fredonia.edu